Amendments to the Claims: This listing of claims will replace all prior versions, and listings, of claims in the application

Listing of Claims:

1. (Currently Amended) An equipment authentication and cryptographic communication system, comprising: user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system, wherein;

(1) said user-end equipment provided with individual user-end equipment information issued by said key center and individual user-end equipment secret information corresponding to said individual user-end equipment's information, and said ~~use-end~~user-end equipment transmits said individual user-end equipment information to said system-end equipment;

(2) said system-end equipment receives said individual user-end equipment information from said user-end equipment, reproduces said individual user-end equipment secret information from said received individual user-end equipment information, and authenticates said user-end equipment by confirming that said user-end equipment legitimately has said individual user-end equipment secret information by using a challenge response utilizing a common key cryptographic algorithm; and

(3) said user-end equipment and said system-end equipment execute a cryptographic communication with each other using said individual user-end equipment secret information.

2. (Original) The equipment authentication and cryptographic communication system according to claim 1, wherein:

(1) said system-end equipment is provided with system-end equipment secret information, which is identical to that possessed by said key center, and produces individual user-end equipment secret information from said individual user-end equipment information using said system-end equipment secret information; and

(2) said user-end equipment authenticates said system-end equipment by confirming that said system-end equipment has said individual user-end equipment secret information by a challenge response utilizing said common key cryptographic algorithm.

3. (Original) The equipment authentication and cryptographic communication system according to claim 1, wherein said system-end equipment is provided with a secret-key cryptographic algorithm, and reproduces said individual user-end equipment secret information by a system conversion of said individual user-end equipment information using a secret key.

4. (Original) The equipment authentication and cryptographic communication system according to claim 3, wherein said system-end equipment and said user-end equipment are both provided with common secret information shared therebetween by exchanging individually held secret information.

5. (Original) The equipment authentication and cryptographic communication system according to claim 4, wherein said system-end equipment and said user-end equipment (a) exchange with each other individually held secret information, and (b) generate new secret information by combining said individually held secret information and said secret information exchanged therebetween according to a predetermined procedure.

6. (Original) The equipment authentication and cryptographic communication system according to claim 5, wherein said system-end equipment and said user-end equipment use said individual user-end equipment secret information for encrypting said new secret information, which is provided by combining said information and said exchanged information.

7. (Original) The equipment authentication and cryptographic communication system according to claim 6, wherein said system-end equipment and said user-end equipment (a) individually generate random digits, (b) exchange said generated random digits with each other, and (c) share the same secret information particular to said system-end equipment and said user-end equipment by combining said generated random digits and said exchanged random digits according to a predetermined procedure.

8. (Original) The equipment authentication and cryptographic communication system according to claim 7, wherein said system-end equipment and said user-end equipment (a) individually generate random digits, (b) combine said random digits with their own information particular to each of said system-end equipment and said user-end equipment according to a predetermined procedure, (c) generate encrypted data by encrypting the combined information using said individual user-end equipment secret information, (d) exchange said encrypted data

with each other, (e) generate decrypted data by decrypting said exchanged encrypted data using said individual user-end equipment's secret information, and (f) reproduce each of said mutually exchanged random digits by dividing the combination of said decrypted data according to a predetermined procedure.

9. (Original) The equipment authentication and cryptographic communication system according to claim 8, wherein said system-end equipment and said user-end equipment (a) individually generate and store random digits, (b) exchange said random digits with each other, (c) combine said exchanged random digits with said individually generated and stored random digits according to a predetermined procedure, (d) generate encrypted data by encrypting said combined information using said individual user-end equipment secret information, (e) exchange said encrypted data with each other, (f) generate decrypted data by decrypting said exchanged encrypted data using said individual user-end equipment secret information, and (g) reproduce each of said mutually exchanged random digits by dividing the combination of said decrypted data according to a predetermined procedure.

10. (Original) The equipment authentication and cryptographic communication system according to claim 9, wherein said system-end equipment and said user-end equipment individually execute matching determinations by comparing said mutually exchanged random digits, which are produced by dividing the combination of said decrypted data according to the predetermined procedure, with said individually generated and stored random digits.

11. (Original) The equipment authentication and cryptographic communication system according to claim 10, wherein said system-end equipment and said user-end equipment produce and store the same data by combining said exchanged and received random digits and said individually generated and stored random digits according to the predetermined procedure, and mutually share said data as a common key particular to both said system-end equipment and said user-end equipment, if said matching determination produces a positive result.

12. (Original) An equipment authentication and cryptographic communication system, comprising: user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system, wherein;

(1) said key center is provided with a first system converter for generating user-end equipment secret information from user-end equipment information;

(2) said user-end equipment is provided with a first storage unit for storing said user-end equipment information provided by said key center, a second storage unit for storing said user-end equipment secret information, a first encryption unit, and a first decryption unit; and

(3) said system-end equipment is provided with a second system converter for generating said user-end equipment secret information by a system conversion of said user-end equipment information received from said user-end equipment, a second encryption unit, and a second decryption unit, and

wherein said user-end equipment and said system-end equipment share and utilize said user-end equipment secret information as a common key for encryption and decryption in said first encryption unit and said first decryption unit in said user-end equipment, and said second encryption unit and said second decryption unit in said system-end equipment.

13. (Original) The equipment authentication and cryptographic communication system according to claim 12, wherein:

(1) said user-end equipment further comprises a first random digit generator for generating a random digit, a second random digit generator for generating a random digit, a first combiner for combining a pair of random digit data according to a predetermined procedure, a first divider for dividing a combined pair of random digit data to reproduce original random digits prior to combining, a first common key generator for combining a pair of random digit data according to a predetermined procedure, and a first matching determination unit for determining if two random digit data match each other; and

(2) said system-end equipment further comprises a third random digit generator for generating a random digit, a fourth random digit generator for generating another random digit, a second combiner for combining a pair of random digit data according to a predetermined procedure, a second divider for dividing a combined pair of random digit data to reproduce original random digits prior to combining, a second common key generator for

combining a pair of random digit data according to a predetermined procedure, and a second matching determination unit for determining if two random digit data match each other.

14. (Original) A method of equipment authentication and cryptographic communication for an equipment authentication and cryptographic communication system including user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system, said method comprising the steps of:

(1) generating user-end equipment secret information from user-end equipment information in said key center;

(2) receiving said user-end equipment information and said user-end equipment secret information in said user-end equipment from said key center;

(3) receiving said user-end equipment information from said user-end equipment, and generating said user-end equipment secret information from said user-end equipment information received in said system-end equipment; and

(4) using said user-end equipment secret information as a common key for encryption and decryption in both of said user-end equipment and said system-end equipment.

15. (Original) The method of equipment authentication and cryptographic communication according to claim 14 further comprising the steps of:

(1) generating a first random digit in said user-end equipment, and transmitting said first random digit to said system-end equipment;

(2) generating a second random digit in said system-end equipment, combining said second random digit and said first random digit received from said user-end equipment, encrypting combined data of said second random digit and said first random digit using said common key, and transmitting said encrypted data to said user-end equipment;

(3) decrypting said encrypted data received in said user-end equipment using said common key, and reproducing said first random digit and said second random digit by dividing decrypted data of said encrypted data received in said user-end equipment;

(4) determining in said user-end equipment if said first random digit reproduced in the preceding decryption step matches with another first random digit generated therein;

(5) generating a third random digit in said user-end equipment, combining said third random digit and said second random digit reproduced in the decryption step, encrypting combined data of said third random digit and said second random digit using said common key, and transmitting encrypted data of said combined data to said system-end equipment;

(6) generating a fourth random digit in said system-end equipment, and transmitting said fourth random digit to said user-end equipment;

(7) combining said fourth random digit received in said user-end equipment from said system-end equipment and said third random digit generated therein, encrypting combined data of said fourth random digit and said third random digit using said common key, and transmitting encrypted data of said combine data to said system-end equipment;

(8) decrypting said encrypted data received in said system-end equipment using said common key, and reproducing said third random digit and said fourth random digit by dividing decrypted data of said encrypted data received in said system-end equipment; and

(9) determining in said system-end equipment if said fourth random digit reproduced in the preceding decryption step matches with another fourth random digit generated therein.

16. (Original) The method of equipment authentication and cryptographic communication according to claim 15 further comprising the steps of:

producing data in said system-end equipment for use as a common key for cryptographic communication by combining said second random digit generated therein with said third random digit reproduced by decryption; and

producing data in said user-end equipment for use as a common key for cryptographic communication by combining said third random digit generated therein and said second random digit reproduced by decryption.

17. (Original) A cryptographic communication system comprising: an IC card, authentication equipment for authenticating said IC card, and intermediary equipment between said IC card and said authentication equipment, wherein;

(1) said IC card includes a first storage unit for storing a secret key particular to said IC card, a second storage unit for storing a certificate of individual IC card key data for generating said secret key, a third storage unit for storing an IC card ID data, and an encryption unit for generating an encrypted data representing response data by encrypting challenge data received from said authentication equipment using said secret key; and

(2) said authentication equipment includes a means for producing said secret key particular to said IC card from said certificate of individual IC card key data received, a first decryption unit for reproducing said response data by decrypting said encrypted data received from said IC card using said produced secret key, and a first matching determination unit for determining if reproduced response data matches said challenge data transmitted by said authentication equipment.

18. (Original) The cryptographic communication system according to claim 17 wherein:

(1) said IC card further includes a receiver for receiving said challenge data generated by said authentication equipment and transmitted via said intermediary equipment, and a response data transmitter for transmitting said encrypted data representing response data, said IC card ID data, and said certificate of individual IC card key data to said authentication equipment via said intermediary equipment;

(2) said means for producing said secret key in said authentication equipment includes a storage unit for storing a validation key, a second decryption unit for producing an IC card ID and a secret key by decrypting said certificate of individual IC card key data received from said IC card, using said validation key; and

(3) said authentication equipment further includes a challenge data generator / storage unit for generating and storing said challenge data, and a second matching determination unit for determining if said response data decrypted by said first decryption unit matches with said challenge data stored in said challenge data generator / storage unit.

19. (Original) The cryptographic communication system according to claim 18 wherein:

(1) said IC card further includes a combiner for generating combined data by combining said IC card ID data, said certificate of individual IC card key data, and said encrypted data, and transmitting said combined data to said authentication equipment; and

(2) said authentication equipment further includes a first divider for dividing said combined data received from said IC card into said IC card ID data, said certificate of individual IC card key data, and said encrypted data, and a second divider for dividing data decrypted by said second decryption unit into said IC card ID and said secret key.

20. (Original) The cryptographic communication system according to claim 19 wherein said authentication equipment further includes a first combiner for combining said challenge data stored in said challenge data generator / storage unit and said IC card ID data produced by said second divider, a third divider for producing said challenge data from data combined by said first combiner, a second combiner for combining said response data decrypted by said first decryption unit and said IC card ID data produced by said second divider, and a fourth divider for producing said response data from data combined by said second combiner.

21. (Currently Amended) An electronic toll collection ("ETC") authentication system including an IC card, roadside equipment, and central processing equipment, comprising:

(1) said IC card including an encryption means for receiving a challenge data generated by roadside equipment, as said IC card passes said roadside equipment, and for encrypting said challenge data using a secret key; an encrypted data storage means for storing data encrypted by said encryption means; a response data transmission means for transmitting IC card ID data and a certificate of individual IC card key data, together with said encrypted data stored in said encrypted data storage means, as response data to said roadside equipment;

(2) said roadside equipment including a dividing means for dividing said transmitted response data ; a second decryption means for decrypting said certificate of individual IC card key data divided by said dividing means, using a validation key; a first matching determination means for making a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by said dividing means; a first decryption means for producing response data by decrypting an encrypted data provided by said dividing means; and a challenge data transmission means for transmitting said challenge data to said IC card; and

(3) said central processing equipment including challenge data storage means for storing said challenge data generated by said roadside equipment; and a second matching determination means for receiving said response data decrypted by said first decryption means, and executing a matching determination of said response data with said challenge data stored in said challenge data storage means,

said ETC authentication system providing authentication of said IC card ID by said roadside equipment by authenticating ~~signature information~~ said certificate of individual IC card key data received with said IC card ID, and said central processing equipment providing a matching determination of said response data, encrypted by said IC card and decrypted by said roadside equipment, to said challenge data.

22. (Currently Amended) An electronic toll collection ("ETC") authentication method comprising the steps of:

(1) encrypting challenge data using a secret key in an IC card, said challenge data being generated by roadside equipment and transmitted to said IC card when said IC card passes by said roadside equipment;

(2) storing said encrypted data;

(3) transmitting an IC card ID data and a certificate of individual IC card key data, in addition to said stored encrypted data, as response data to said roadside equipment;

(4) dividing said response data received by said roadside equipment ;

(5) decrypting said certificate of individual IC card key data, provided by the dividing step, using a validation key;

(6) carrying out a matching determination of an IC card ID provided in the decrypting step with another IC card ID provided in the dividing step;

(7) providing a response data by decrypting said encrypted data provided in the dividing step; and

(8) carrying out in said central processing equipment a matching determination of said response data decrypted by said roadside equipment with said challenge data,

said ETC authentication method providing authentication of said IC card ID by said roadside equipment by authenticating ~~signature information~~said certificate of individual IC card key data received with said IC card ID, and said central processing equipment providing a matching determination of said response data encrypted by said IC card and decrypted by said roadside equipment.

23. (Currently Amended) An electronic toll collection ("ETC") authentication system comprising:

(1) first roadside equipment including challenge data and time generator / storage means for generating and storing challenge data and time information, and transmitting said challenge data and time information to an IC card;

(2) said IC card including an ID transmission means for transmitting an IC card ID before said IC card passes said first roadside equipment; an encryption means for receiving said challenge data and said time information generated by said first roadside equipment, as said IC card passes said first roadside equipment, and encrypting received data using a secret key; a response data transmission means for transmitting an IC card ID data and a certificate of individual IC card key data, together with said encrypted data as a response data to a second roadside equipment;

(3) said second roadside equipment including a first dividing means for dividing said response data ; a second decryption means for decrypting said certificate of individual IC card key data divided by said first dividing means, using a validation key; a first matching determination means for providing a matching determination of an IC card ID produced as a result of decryption with another IC card ID provided by said first dividing means; and a first decryption means for producing a response data by decrypting an encrypted data obtained from said first dividing means; and

(4) central processing equipment including a second dividing means for dividing said challenge data and said IC card ID generated by said first roadside equipment; a third dividing means for dividing said response data and said IC card ID decrypted by said second roadside equipment; and a second matching determination means for making a matching determination of said challenge data obtained by said second dividing means and said response data provided by said third dividing means,

said ETC authentication system providing authentication of said IC card ID by said second roadside equipment by authenticating ~~signature information~~said certificate of individual IC card key data received with said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment.

24. (Original) The ETC authentication system according to claim 23, wherein said second roadside equipment further comprises another decryption means for decrypting said encrypted data provided by said first dividing means, using a secret key reproduced by said second decryption means; and a validation means for providing time information, at which said IC card passed said first roadside equipment, from a decrypted result of said another decryption means, and for confirming if a difference between said time information and present time is within a predetermined time period.

25. (Currently Amended) An electronic toll collection ("ETC") authentication method comprising the steps of:

(1) receiving a card ID from an IC card before said IC card passes first roadside equipment;

(2) encrypting challenge data and time information using a secret key, said challenge data and time information being generated by first roadside equipment and transmitted to said IC card when said IC card passes said first roadside equipment;

(3) transmitting IC card ID data and a certificate of individual IC card key data, in addition to said encrypted data, as a response data to second roadside equipment;

(4) dividing said transmitted response data in said second roadside equipment;

(5) decrypting said certificate of individual IC card key data provided in the dividing step using a validation key;

(6) carrying out a matching determination of an IC card ID provided in the decryption step with another IC card ID provided in the dividing step;

(7) providing a response data by decrypting said encrypted data provided in the dividing step;

(8) carrying out in central processing equipment a matching determination of said challenge data provided from said first roadside equipment and said response data decrypted in said second roadside equipment,

said ETC authentication method providing authentication of said IC card ID by said second roadside equipment by authenticating ~~signature information~~said certificate of individual IC card key data received with said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment.

26. (Original) The ETC authentication method according to claim 25 further comprising the steps of:

(1) decrypting said encrypted data provided by the dividing step, using a secret key reproduced in said decryption step; and

(2) providing time information, at which said IC card passed said first roadside equipment, as a result of the decryption step, and confirming if a difference between said time information and present time is within a predetermined time.

27. (Currently Amended) An electronic toll collection ("ETC") authentication system comprising:

(1) a first roadside equipment including a challenge data generation means for generating a challenge data, and transmitting said challenge data to an IC card;

(2) said IC card including an ID transmission means for transmitting an IC card ID before said IC card passes said first roadside equipment; an encryption means for receiving said challenge data generated by said first roadside equipment, as said IC card passes said first roadside equipment, and encrypting said challenge data using a secret key; and a response data transmission means for transmitting an IC card ID data and a certificate of individual IC card key data, together with said encrypted data as response data to second roadside equipment;

(3) said second roadside equipment including a first dividing means for dividing said response data; a decryption means for decrypting said certificate of individual IC card key data divided by said first dividing means, using a validation key; a first matching determination means for providing a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by said first dividing means; and a first decryption means for decrypting an encrypted data provided by said first dividing means to obtain response data;

(4) central processing equipment including a second dividing means for dividing said challenge data and said IC card ID generated in said first roadside equipment; a third dividing means for dividing said response data decrypted in said second roadside equipment and said IC card ID; and a second matching determination means for providing a matching determination of said challenge data obtained in said second dividing means and said response data obtained in said third dividing means,

said ETC authentication system providing authentication of said IC card ID by said second roadside equipment by authenticating ~~signature information~~said certificate of individual IC card key data received with said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment.

28. (Currently Amended) An electronic toll collection ("ETC") authentication method comprising the steps of:

(1) receiving a card ID from an IC card before said IC card passes by first roadside equipment;

(2) encrypting a challenge data using a secret key, said challenge data being generated by said first roadside equipment and transmitted to said IC card when said IC card passes said first roadside equipment;

(3) transmitting each individual data of said IC card ID and a certificate of individual IC card key data, in addition to said challenge data encrypted in the encryption step, as response data to second roadside equipment;

(4) dividing said response data transmitted in the transmission step by said second roadside equipment;

(5) decrypting said certificate of individual IC card key data divided in the dividing step, using a validation key;

(6) carrying out a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by the dividing step;

(7) producing a response data by decrypting said encrypted data provided by the dividing step; and

(8) executing in central processing equipment a matching determination of said challenge data provided by said first roadside equipment and said response data decrypted by said second roadside equipment,

said ETC authentication method providing authentication of said IC card ID by said second roadside equipment by authenticating ~~signature information~~said certificate of individual IC card key data received said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment.